#20

OFFICIAL

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Appellant: Gorkem I. Ates

Series Code/Serial No.: 09/401,221 Filed: September 22, 1999

Group Art Unit: 2152 Paper No.: 20

Invention: INTERNET SYSTEM

Examiner: Hai V. Nguyen Agent's Doc. No.: ATEG21A

As article No.: EL586861_|_|_|_|US EXPRESS MAIL I hereby certify, that on or before the below indicated date, this correspondence is being deposited with the United States Postal Service with sufficient postage in an envelope addressed to the: Commissioner for Patents, P.O. BOX 1450, Alexandria, VA 22313-1450, and/or facsimile (703-872-9306) transmitted to the U.S. Patent and Trademark Office.

MAIL STOP Appeal (PATS)
Commissioner for Patents
P.O. BOX 1450
ALEXANDRIA, VA 22313-1450

BY: Richard L. Miller
Agent for Appellant

Date: April 27, 2004

copy #3

REPLY BRIEF

Sir:

Appellant files the instant Reply Brief in triplicate.

The Examiner states at page 14, paragraph 2 of the Examiner's Answer that:

> "The examiner has already shown and replied in the last Office Action (paper #15). Appellant's only argument is 'a WAN is not equivalent to the Internet' (Appellant's Brief, pages 25-26). The Internet and the Wide Area Network (WAN) are types of communication medium used. Therefore, the communication medium used (the Internet or the WAN) is relevant to execute the functionalities of the limitations of the claimed invention."

Appellant disagrees. Appellant respectfully resubmits that a WAN is not equivalent to the Internet and is NOT relevant to execute the functionalities of the limitations of the claimed invention as will be shown infra.

A WAN (Wide Area Network) is a network which can be utilized over relatively long distances, quite often between buildings and some times transmitted over telephone lines or with a satellite transmission system. Protocol can be what ever is agreed upon. Some common protocols include TCP/IP, NetBEUI, IPX/SPX-compatible Protocol, WAN support for ATM, ATM Call Manager, etc. The Internet, however, only permits TCP/IP protocol, and is the largest WAN of all. Therefore, even though the Internet is a WAN, a WAN is not necessarily the Internet. There is no reciprocity between A WAN and the Internet. The Internet is not equivalent to Wide Area Network.

Support for assertion that the Internet is not equivalent to a Wide Area Network can be found in the declaration of Gary J. Levanti under 37 CFR 1.68 in lieu of affidavit under 35 CFR 1.132 traversing grounds of rejection by distinguishing Internet is not equivalent to Wide Area Network from each other submitted with appellant's Brief.

Further support for this assertion can be found in In re Gosteli, 872 F.2d 1008, 10 USPQ.2d 1614 (Fed. Cir. 1989), where the Court held:

> "...species rejects genera, but the converse is not necessarily so." [Emphasis added]

In applying the decision of the Gosteli Court, it is revealed that a WAN is a genus which cannot reject the specie of the Internet.

With Brendel et al's use of a WAN instead of the Internet, the server 52 cannot be located anywhere in the world regardless of where in the world the load balancer 70 is located ipso facto the load balancer 70 communicates with the server 52 over the discrete and/or distinct and/or dedicated connection 120.

Additionally, Brendel et al. disclose at col. 20, lines 34-37:

> "The web farm has been described as having a "local" network, but this local network could be local only in the sense that it is not the Internet backbone."

Brendel at al. teach communicating between the scheduler and the server with a proprietary (OSI 3rd level) protocol called IXP.

In contradistinction, the present invention teaches communicating with the participants (the equivalent of web servers in Brendel et al.) from the main server (the scheduler) with the standard IP (Internet Protocol) protocol so that the present invention can reside where there is no specialized frame relay or ISDN or leased line communication between the scheduler and the participant and when there is only a standard Internet connection that is using the Internet backbone, which Brendel et al. simply cannot do. The at least one participant server can be located anywhere in the world regardless of where in the world the main server is located.

The present invention is a system and method for allowing TCP/IP servers to assign jobs to other servers dynamically without relocating the client using neither HTTP nor HTML commands, wherein the "main server" is the server of the ISP (the main TCP/IP server), the "participants" are the servers that are assigned jobs, and the "client" is the client computer that makes the actual request. The system and method of the present invention depend upon the publicly known technique of "IP Spoofing" and take the relocating process away from the top networking OSI layers, such as TCP, HTTP and application level to the 3rd level of internetworking OSI that is the IP. It enables Internet-wide load balancing and content delivery with only a single IP involved as the listener.

In practice, the client requests a file or document from the main server (a streaming video and/or audio file is typical).

The main server operates at the firewall/IP level and has an IP stack (separate from the TCP/IP stack of the operating system) that can forward packets to another host with a TCP/IP connection and a basic

database running that stores and retrieves the data of IP addresses and the ports of the participant servers and the socket information (IP, port, latest sequence number of the packet exchange as well as the TCP state) of the client. The main server examines the client's IP address and seeks the nearest participant server (the one that has the most bandwidth and CPU, geographically closest, and other serving requirements needed to serve a document to the client).

The main server, acting like an orchestra chief, requests the participant to send the document client requested to the client packet-by-packet, labeling each packet with the senders IP address being the main servers IP address. This enables the client, which has a port open only for a main server's address to accept the packets (the file). To accomplish this goal, the main server examines the IP address port of the packet. Then takes action as;

1. If the port of the specific client's socket does not have a correspondence in the database (determined after a "SELECT" SQL statement), which means that the client has just started a connection with a SYN packet. Then this client socket is stored in the database with four variables: IP address, port number, and TCP state along with a timestamp for the socket; and
2. If the IP and port are present in the database as an active connection (a connection that is transferring data or in a wait state but not terminated), then the timestamp of the socket is updated with the current time of the arrival of the latest packet.

The purpose of the timestamp is for a background thread in the main server to clean the obsolete (closed) socket entries in the database. The background thread does this by subtracting the timestamp from the current time and comparing this value with a defined (by the main server programmer or administrator) timeout value. If the timeout value is exceeded then the database entry is deleted. This means that the socket is indeed broken.

After that, the packet is modified. The source IP and port of the packet are preserved. The destination IP and port of the packet are changed to the listening IP and the port of the participant is selected as being geographically closest and with the best free resources in terms of CPU usage, volatile and non-volatile memory, and bandwidth.

The participant server processes the request as if it was directly requested by the client since the participant does not know from the IP packet that it was routed from the main server and thinks that the packet actually comes from the client since the packet has the source IP of the client. The participant sends the requested object with the sender's address (source IP) of the main server's IP address at the IP level. This may require root privileges under Linux. Other requirements may apply to other systems.

When the client makes another request using the main server's IP address, the client requesting packages are routed to the main server, NOT to the participant server. This is the "normal behavior" of today's networking equipment (i.e. routers) and software.

In live stream and the participant does not have the file requested, than the file is first downloaded to the participant and than sent to the clients. In the lack of multicasting this will distribute the load of the main server to the participant servers and thus would save costs because adding participant servers would be relatively easy and cheap to add than clustering more servers to the main server.

The present invention:

1. Provides the advantages of multicasting such as low server and bandwidth costs but without multicasting supporting hardware.
2. Is fast and flexible - the number of participants can be changed dynamically with little cost compared to upgrading the main server.
3. Is not difficult to implement.
4. Relies on the fact that multicasting equipment is expensive and ISP's are reluctant to upgrade and unless most of the net is equipped with multicasting machines, multicasting won't operate efficiently.
5. Participants are safe in the network against attacks such as denial of service attacks because their IP addresses are not revealed to the clients, and thus hackers.

In operation,

a main server is established. A participant Internet surfer enters username, password, and other necessary information required for financial processing to a form in a web page of the website of the present invention. When a participant user decides to become active in the system, it will surf to the website and enter his username, password. The

participant's computer will then load an applet (possibly written in ActiveX or Java in 1999 terms) that will be the server software of the "participant" (participant is the participating web surfer or company computer). The applet will first calculate the participants CPU, bandwidth, and memory power (and other necessary resources) and will start a timer for the participant to start serving under rule of the main server. Information about the participant will be recorded on a database in the main server (main server may be any machine with at least one IP address connected to the Internet backbone). When a web surfer requests a file, the main server will search through its database of servers and select the most appropriate server in terms of serving ability depending on its previous evaluation of participants. The main server will command the participant, via the open listening socket of the applet loaded in the participant's machine, to serve the client. When the participant server decides to go offline, the main server calculates the amount earned by the participant Internet user and records it. At the end of a period, participant person will get his money by check. The main server will have the computing power of the net efficiently, cheaply, and dynamically at its fingerprints. The main server will be the powerhouse between ISPs.

RICHARD L. MILLER
12 Parkside Drive
Dix Hills, NY 11746-4879

PHONE (631) 499-4343

RESPECTFULLY SUBMITTED

Richard L. Miller
Agent for Appellant

Date: April 27, 2004